UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/742,705	12/20/2000	Juha Salokannel	460-009952-US(PAR)	9125

7590 04/03/2009

Clarence A. Green
Perman & Green, LLP
425 Post Road
Fairfield, CT 06430

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
04/03/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/742,705	SALOKANNEL, JUHA	
	Examiner	Art Unit	
	MATTHEW T. HENNING	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 January 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

This action is in response to the communication filed on 1/27/2009.

DETAILED ACTION

Response to Arguments

Applicant's arguments filed 1/27/2009 have been fully considered but they are not persuasive, in view of the new grounds of rejection presented below, which was necessitated by the amendments to the claims.

Regarding the applicant's argument that "Dent uses the whole keystream of bits" and therefore does not perform selection between encryption keys, the examiner does not find the argument persuasive. In this case, each N block of bits in an encryption key, as disclosed by Dent in Col. 13 Paragraph 2. The selection of the encryption key occurs by generating the keystream block using the block counter. The keystream itself is the set of encryption keys. The keystream contains many N blocks of bits, and each N-bit block is an encryption key. It is selected the block counter by using the "generator" to output the N-bit block encryption key. Furthermore, the claims do not recite that "only one key is selected". As such, the examiner does not find the argument persuasive.

Regarding the applicant's argument that "the Examiner apparently believes that because the N bits may contain variable bit patterns, they all can be regarded as encryption keys", the examiner does not agree. The N-bit blocks are each encryption keys because each N-bit block is used to encrypt a frame of traffic.

Regarding the applicant's argument that because Dent mentions "broadcasting", that Dent is implying that the transmission is intended for several mobile stations, the examiner does

not find the argument persuasive. This is because "broadcasting" simply means transmitting the data using radio waves. As such, the examiner does not find the argument persuasive.

Regarding the applicant's argument that col. 6 lines 46-51 "supports the view that the low data rate control channel is used as a general broadcast channel", the examiner does not find the argument persuasive. This section cited by the applicant recites that "synchronization information is periodically transmitted on a low data rate channel from said base stations to the mobile stations". It does not state that "a single counter value" (the counter value is what is being relied upon as reading on the "data about the encryption key" is transmitted from the base station to the mobile stations. The cited section is not specific enough in description to determine whether each mobile station receives a separate counter value. As such, the applicant's argument is not found persuasive. Further, note that in rejecting the claims below, the FACCH is being relied upon as the channel, and not the previously relied upon SACCH.

Regarding the applicant's argument that Dent disclosing "resuming transmission of cryptographically encoded message traffic data bits from the second base station to the mobile station" must mean that the synchronization information sent over the FACCH is intended for several mobile terminals, the examiner does not find the argument persuasive. While the examiner appreciates the applicant's interpretation of the disclosure of Dent, the examiner disagrees with the applicant. Because this is a handoff, and cryptographically encoded message traffic had been sent from the first base station to the mobile station, the new base station can "resume" the cryptographically encoded message traffic, and does so after transmitting the counter value to the mobile station on the FACCH for a predetermined period of time. Nowhere in Dent is it disclosed or suggested that the FACCH, or the data contained therein, is "intended

for several mobile terminals". In fact, throughout Dent, it is clear that the synchronization information transmitted in the FACCH is transmitted from the second base station to "the mobile station [being handed off]". Further still, as previously argued, the FACCH is not a "general control channel" and further it is not "intended for several mobile terminals". As such, the examiner does not find the argument persuasive.

Regarding the limitation of "transmitting from the second access point, at intervals, data about the encryption key selected at the time over a broadcast control channel to the mobile terminal", the examiner points out that this limitation has been addressed below in the new rejection presented below, as due to the amendment to the claims, the SACCH no longer read on the claimed broadcast control channel. Note that in rejecting the claims, the FACCH is now relied upon as reading on the broadcast control channel.

Further note that "at intervals" does not mean "periodically".

All rejections and objections not presented below have been withdrawn.

Claims 1-21 have been examined.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-5, 8, 9-13, 16, and 18-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dent (U.S. Patent 5,081,679) hereinafter referred to as Dent.

Regarding claim 1, Dent disclosed a method comprising: defining a set of encryption keys comprising at least two encryption keys (N-bit blocks of keystream data) (See Dent Col. 5 Lines 51-57 wherein the keystream is the "set" of keys and the blocks of keystream data, see col. 13 lines 27-30 and 35-39, are the keys in the set), selecting at each of first and second access points (BS) from said set of encryption keys one encryption key (N-bit block) at a time for encrypting information to be transmitted between said first and second access points and a mobile terminal (MS) (See Dent Col. 5 Lines 57-66), transmitting from the second access point, data about the encryption key selected at the time over a broadcast control channel (high data rate channel FACCH) to the mobile terminal (See Dent Col. 15 Lines 2-8), setting up a data transmission connection between said mobile terminal and the first access point for the transmission of information (See Dent Col. 6 Lines 5-8 and Col. 6 Lines 45-61), and performing a handover, to set up a data transmission connection between the second access point and the mobile terminal (See Dent Col. 6 Lines 12-15, 30-39), wherein in connection with the handover, said data is transmitted over said broadcast control channel to the mobile terminal about the encryption key selected at the second access point (See Dent Col. 15 Lines 2-8), and for the transmission of information said data about the encryption key such a broadcast control channel control field is selected which is not used as a general broadcast control channel control field intended for several mobile terminals (See Dent Col. 6 Line 45 – Col. 7 Line 2 and Col. 10

Paragraph 3), but Dent did not specifically disclose that the data about the encryption key was transmitted at intervals over the broadcast control channel.

However, Dent did disclose in Col. 15 Lines 2-8 that after a certain number of FACCH transmissions of the synchronization information, the base station ceases further FACCH transmissions of the synchronization information. This implies that the synchronization information was transmitted multiple times, and therefore "at intervals". As such, it would have been obvious to the ordinary person skilled in the art at the time of invention to have transmitted the synchronization information over the FACCH at intervals. This would have been obvious because the ordinary person skilled in the art would have been motivated to transmit the synchronization information “a certain number of times” throughout the set "timeout" period of time, as disclosed by Dent.

Regarding claims 9 and 19-21, Dent disclosed a mobile communication system comprising: at least one mobile terminal (MS), at least a first access point and a second access point (BS); a set of encryption keys being defined in the communication system (See Dent Col. 5 Lines 51-57 wherein the keystream is the “set” of keys and the blocks of keystream data, see col. 13 lines 27-30 and 35-39, are the keys in the set); each of the access points comprising a circuit for selecting from said set of encryption keys (keystream) one encryption key (N-bit Block) at a time to be used for encryption of information to be transmitted between each of said access points and said mobile terminal (See Dent Col. 5 Lines 57-66), and a circuit for transmitting data about the encryption key selected at the time at intervals from the second access point over a broadcast control channel (high data rate channel FACCH) to the mobile terminal (See Dent Col. 15 Lines 2-8); the communication system also comprising: a circuit for setting up a data

transmission connection between the mobile terminal and the first access point for the transmission of information (See Dent Col. 6 Lines 5-8 and Col. 6 Lines 45-61), and a circuit for executing a handover and setting up a data transmission connection between the second access point and the mobile terminal (See Dent Col. 6 Lines 12-15, 30-39), wherein the mobile communication system also comprises a circuit for transmitting over said broadcast control channel (FACCH) said data about the encryption key selected at the second access point to the mobile terminal in connection with the handover (See Dent Col. 6 Lines 45-61), and said circuit for transmitting is configured to select for the transmission of said data about the encryption key such a broadcast control channel control field which is not used as a general broadcast control channel control field intended for several mobile terminals (See Dent Col. 6 Line 45 – Col. 7 Line 2 and Col. 10 Paragraph 3), but Dent did not specifically disclose that the data about the encryption key was transmitted at intervals over the broadcast control channel.

However, Dent did disclose in Col. 15 Lines 2-8 that after a certain number of FACCH transmissions of the synchronization information, the base station ceases further FACCH transmissions of the synchronization information. This implies that the synchronization information was transmitted multiple times, and therefore "at intervals". As such, it would have been obvious to the ordinary person skilled in the art at the time of invention to have transmitted the synchronization information over the FACCH at intervals. This would have been obvious because the ordinary person skilled in the art would have been motivated to transmit the synchronization information “a certain number of times” throughout the set "timeout" period of time, as disclosed by Dent.

Regarding claims 2 and 10, Dent disclosed that each encryption key in said set of encryption keys is allocated an encryption number (Block Counter Number), and said encryption number is used as said data about the encryption key selected (See Dent Claims 32-34).

Regarding claims 3 and 11, Dent disclosed information is transmitted in data frames, wherein the encryption key is changed in connection with each data frame (See Dent Col. 10 Lines 14-17).

Regarding claims 4 and 12, Dent disclosed that some of the data frames are used as common data frames for transmitting information from the second access point to more than one mobile terminal, wherein said data about the encryption key is transmitted in another data frame than said common data frame (See Dent Col. 8 Line 54 – Col. 9 Line 5).

Regarding claims 5 and 13, Dent disclosed said set of encryption keys is stored in said access points and in the mobile terminal (See Dent Col. 5 Lines 51-57).

Regarding claims 8 and 16, Dent disclosed that the first access point executes a forced handover, in which the mobile terminal communicating with said first access point is transferred to communicate with said second access point, said first access point transmits information about the handover to said second access point, and said second access point transmits said data about the encryption key selected at the second access point at the time to the mobile terminal. (See Dent Col. 6 Lines 12-22).

Regarding claim 17, Dent disclosed that said encryption keys are frame specific (See Dent Col. 10 Lines 14-17), and are generated at both ends of said transmission connection (See Dent Figs. 2-3 Elements 115 and 115', Col. 8 Lines 54-57, Col. 10 Lines 14-17, Col. 11 Lines 39-41, and Col. 12 Lines 23-32).

Claims 6 and 14 rejected under 35 U.S.C. 103(a) as being unpatentable over Dent as applied to claim 1 and 9 respectively above, and further in view of Kojima et al. (U.S. Patent Number 5,323,446) hereinafter referred to as Kojima.

Dent disclosed handing off a MS from a first BS to a second BS (See Dent Col. 6 Lines 12-15). However, Dent failed to disclose that the MS could initiate the handoff. Dent also disclosed that during this handoff, the voice channel is seized for authentication purposes and no longer sends voice data (See Dent Col. 12 Paragraph 4).

Kojima teaches that if the mobile terminal requests the handoff to both the old and the new base station, then the handoff can ensure transparency to the data signals (See Kojima Summery of the Invention).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Kojima in the invention of Dent by having the mobile terminal send handoff requests to both the old and new base stations. This would have been obvious because one skilled in the art would have been motivated to preserve data integrity in the communication.

It would have been obvious in the combination of Dent and Kojima that the new base station sent its synchronization information to the mobile terminal at the time of handoff request. This would be obvious because the ordinary person skilled in the art would have been motivated to enable the mobile terminal to communicate securely with the new base station.

Claims 7 and 15 rejected under 35 U.S.C. 103(a) as being unpatentable over Dent as applied to claim 1 and 9 respectively above, and further in view of Gilhousen et al. (U.S. Patent Number 5,101,501) hereinafter referred to as Gilhousen.

Dent disclosed handing off a MS from a first BS to a second BS (See Dent Col. 6 Lines 12-15), but Dent failed to disclose that the MS could initiate the handoff. However, Dent disclosed the handoff signal originating at the old base terminal (See Dent Col. 6 Lines 12-15).

Gilhousen teaches that by providing the mobile unit with the ability to detect the need for handoff, the mobile unit can become more aware of its possible communication paths much sooner and with less effort than if the information was relayed from its base station, which allows the mobile unit to find the cell site with the strongest signal and request handoff to that cell (See Gilhousen Col. 8 Paragraphs 4-5).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Gilhousen to the invention of Dent by having the mobile unit detect the need for a handoff and then request the handoff. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide the mobile terminal with the strongest signal available.

It would have been obvious in the combination of Dent and Gilhousen that the new base station sent its synchronization information to the mobile terminal at the time of handoff request. This would be obvious because the ordinary person skilled in the art would have been motivated to enable the mobile terminal to communicate securely with the new base station.

Conclusion

Claims 1-21 have been rejected.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MATTHEW T. HENNING whose telephone number is (571)272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Matthew T Henning/
Examiner, Art Unit 2431

/Ayaz R. Sheikh/

Supervisory Patent Examiner, Art Unit 2431